(12) UK Patent Application (19) GB (11) 2 342 744 (13) A

(43) Date of A Publication 19.04.2000

(21) Application No 9920744.1

(22) Date of Filing 02.09.1999

(30) Priority Data
(31) 10292153 (32) 14.10.1998 (33) JP

(71) Applicant(s)
Kabushiki Kaisha Toshiba
(Incorporated in Japan)
72 Horikawa-cho Saiwai-ku, Kawasaki-shi,
Kanagawa-ken, Japan

(72) Inventor(s)
Miki Yamada
Tomoaki Morijiri

(74) Agent and/or Address for Service
Batchellor, Kirk & Co
102-108 Clerkenwell Road, LONDON, EC1M 5SA,
United Kingdom

(51) INT CL[7]
G06F 1/00 , G07C 9/00 , H04M 1/66

(52) UK CL (Edition R)
G4H HTG H1A H13D H14A H14D
G4A AAP
H4K KOE
U1S S2125 S2215

(56) Documents Cited
GB 2148569 A WO 93/13518 A1

(58) Field of Search
UK CL (Edition Q) G4A AAP , G4H HTG , H4K KBHG KF50C KOE
INT CL[6] E05B , G06F , G07C , H04M

(54) Abstract Title
User confirmation using biometrics

(57) A user confirmation system using biometrics includes a plurality of types of user confirmation execution sections for confirming a user in accordance with different methods,respectively, and presents the user confirmation methods so the user can select which will be used. The user confirmation system can flexibly cope with an emergency that disables use of a given user confirmation section.

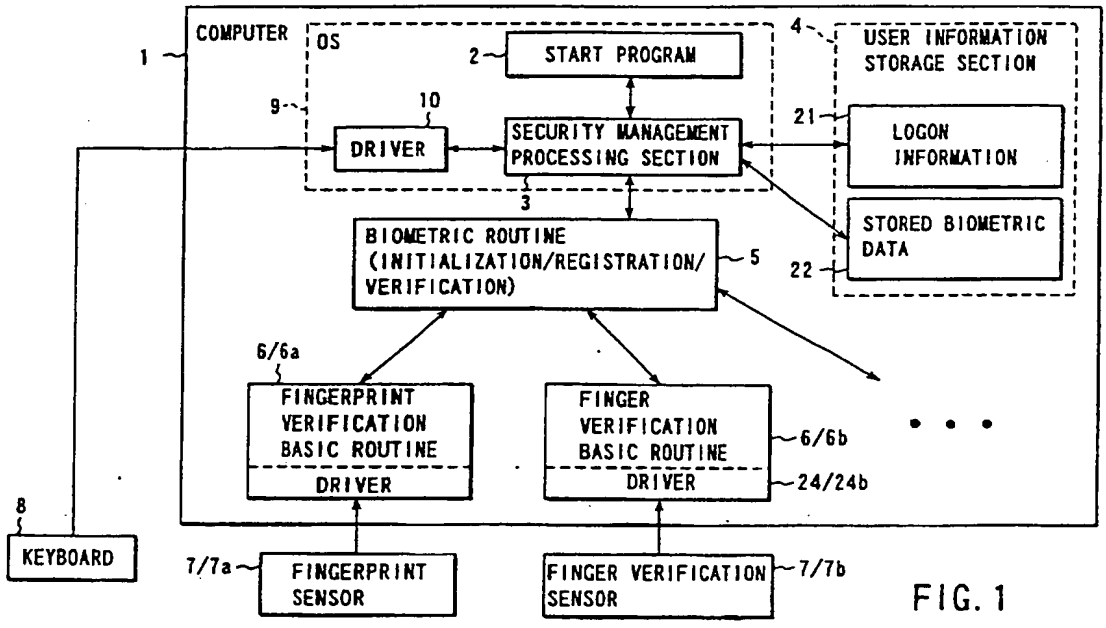

FIG. 1

GB 2 342 744 A

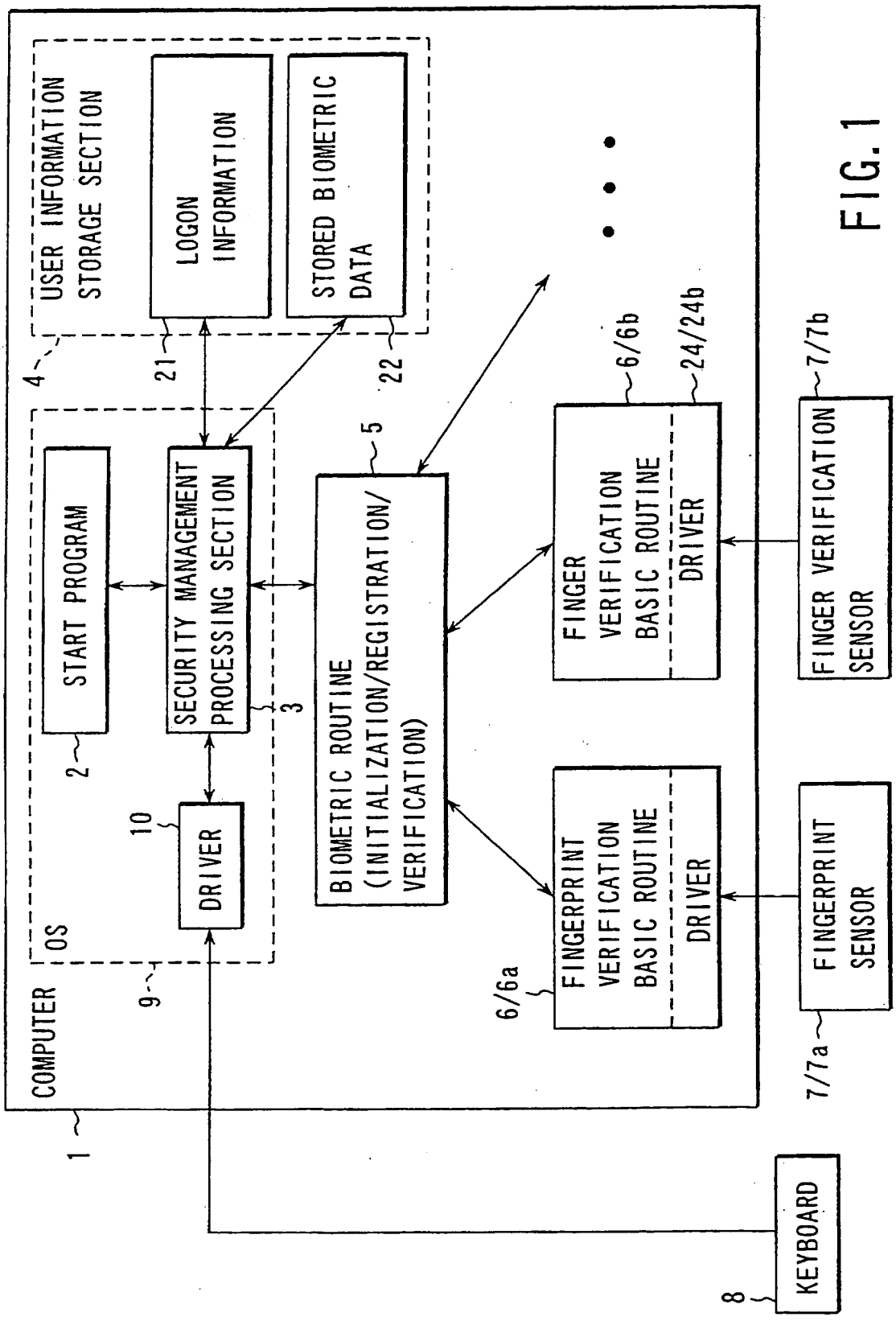

FIG. 1

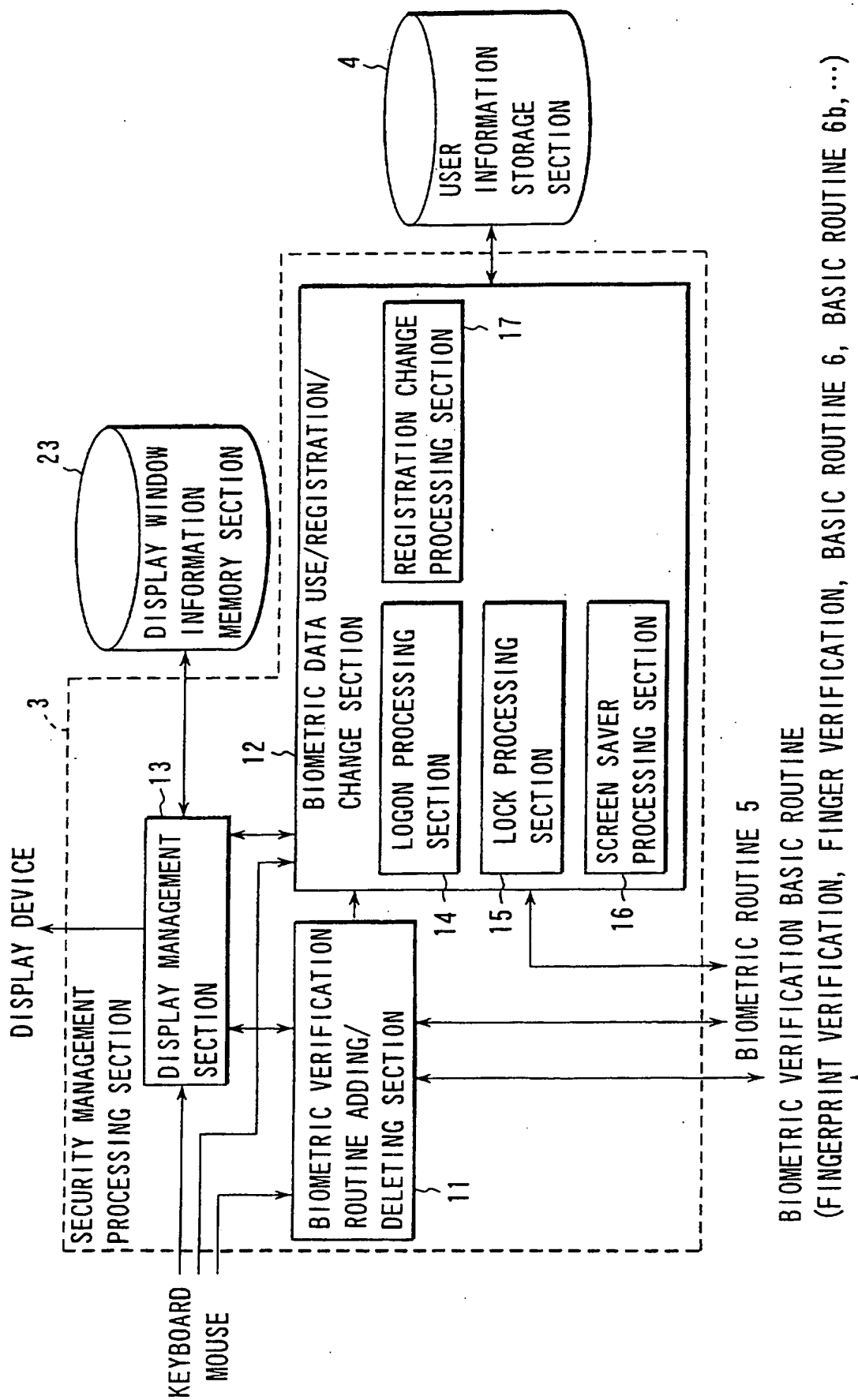

FIG. 2

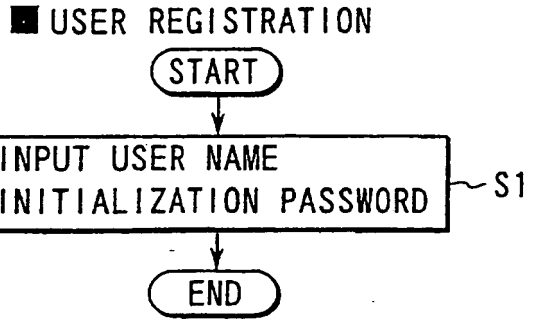

FIG. 3

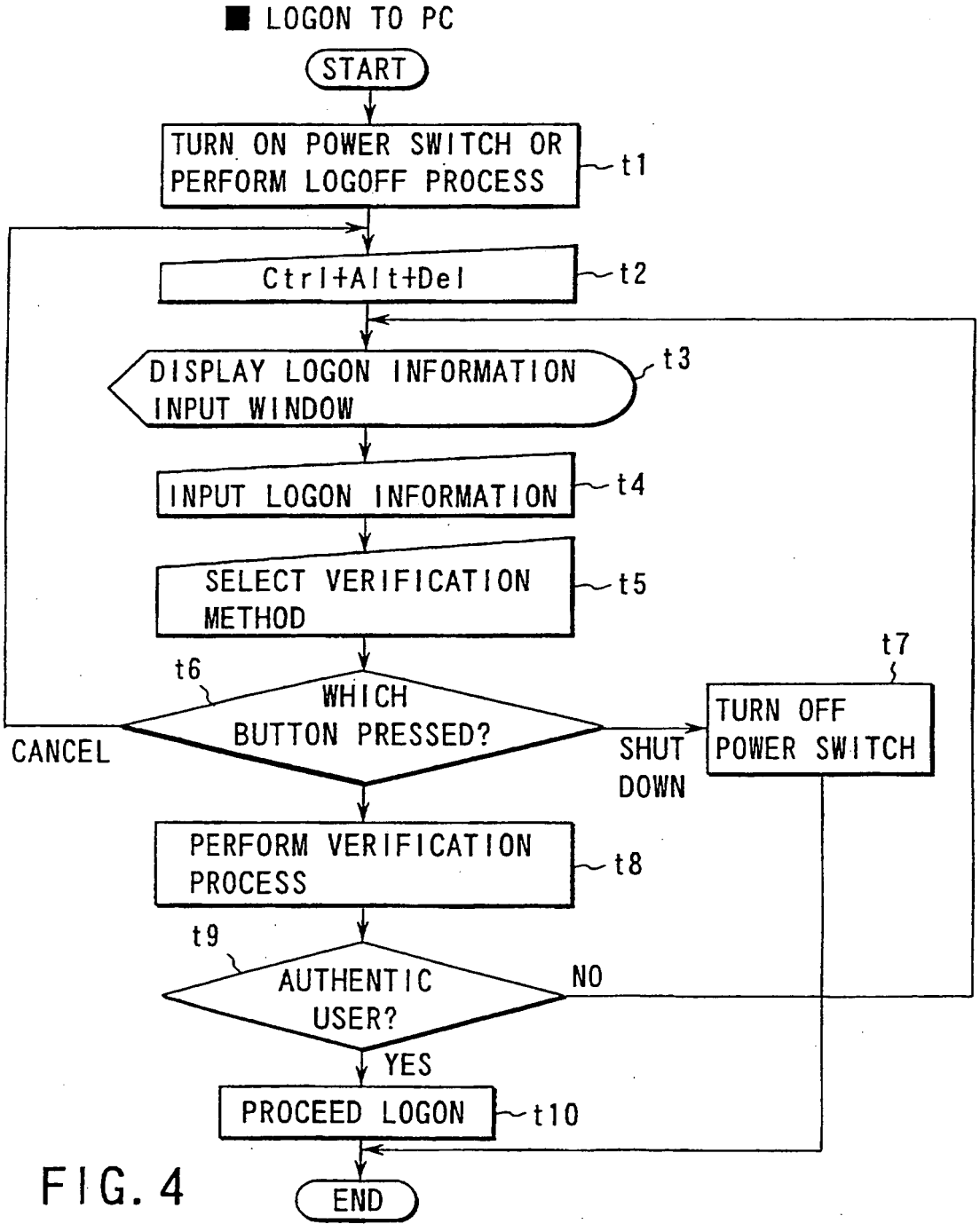

FIG. 4

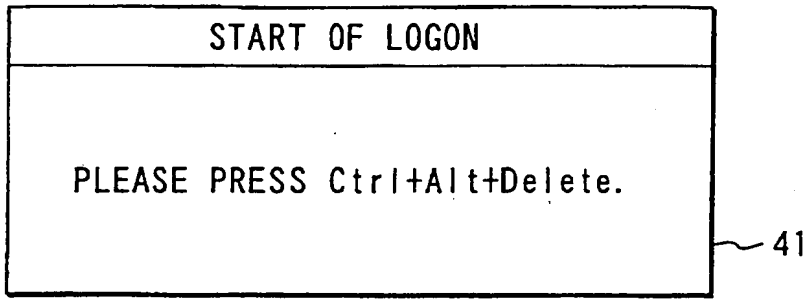

FIG. 5

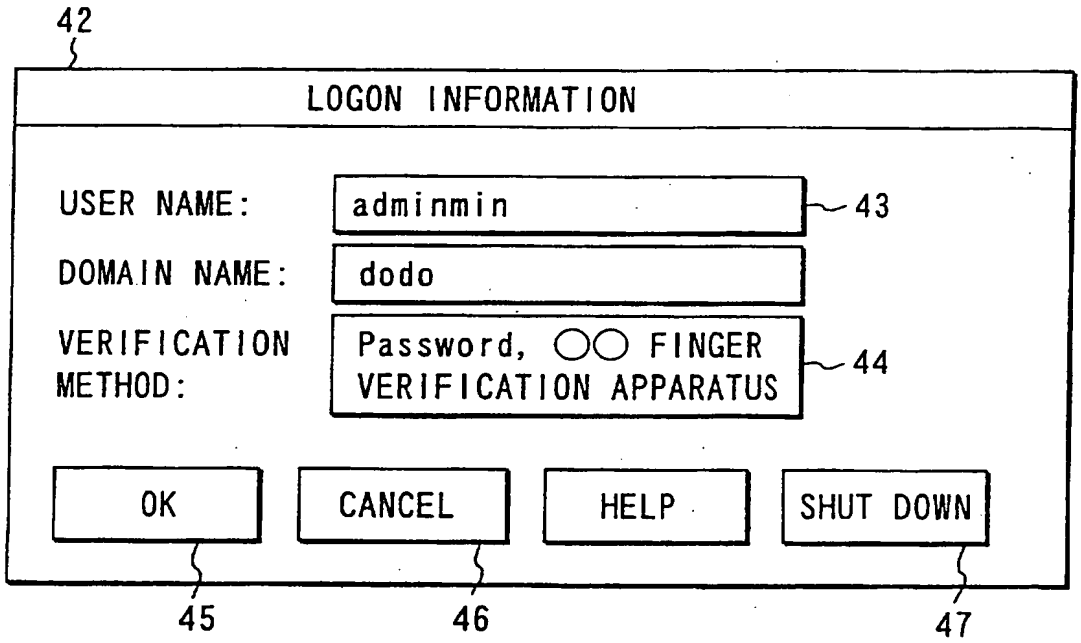

FIG. 6

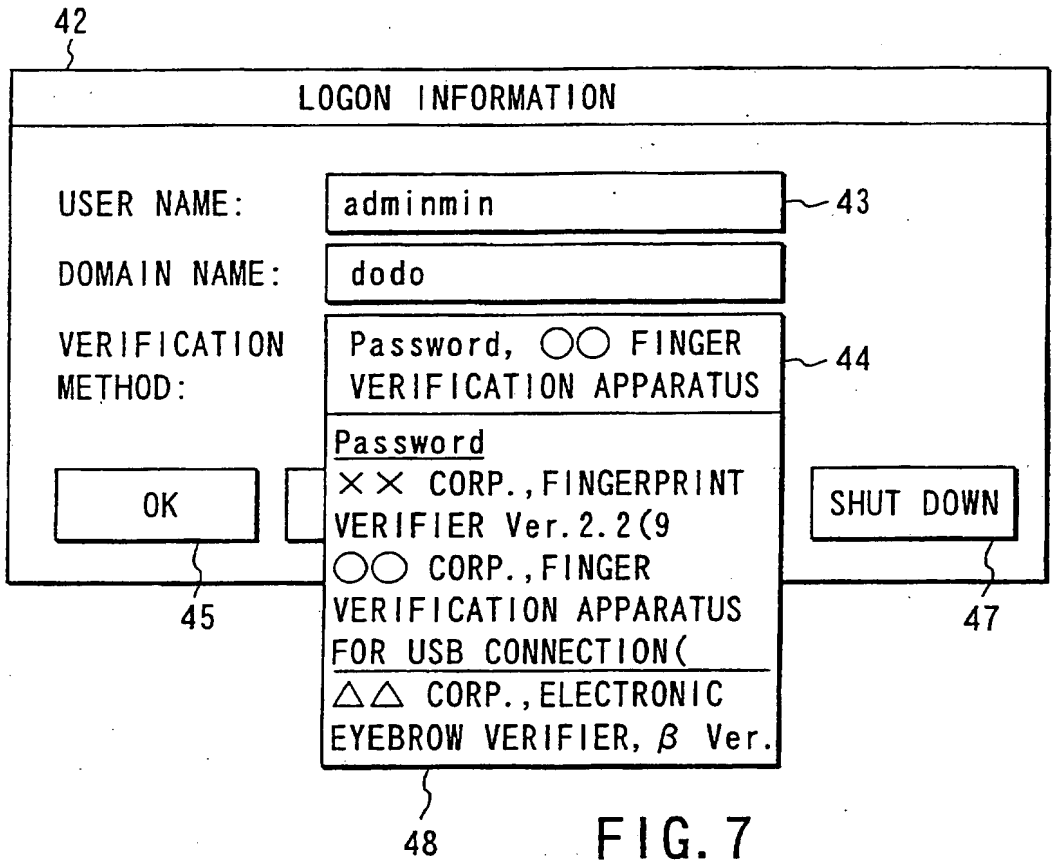

FIG. 7

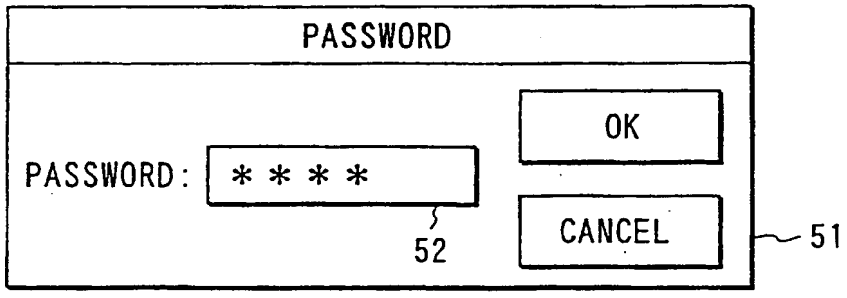

FIG. 8

■ REGISTRATION / CHANGE OF BIOMETRIC DATA

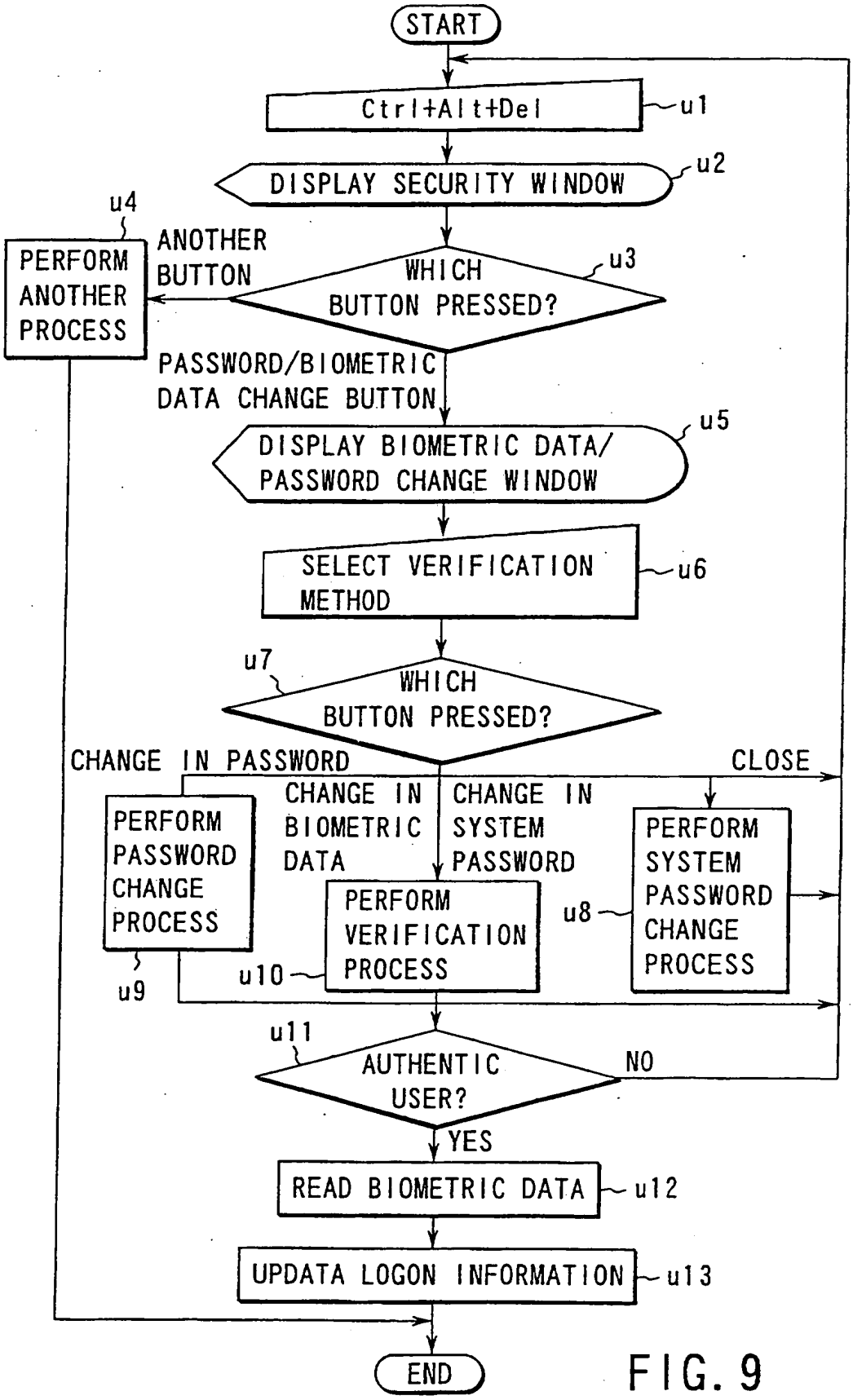

FIG. 9

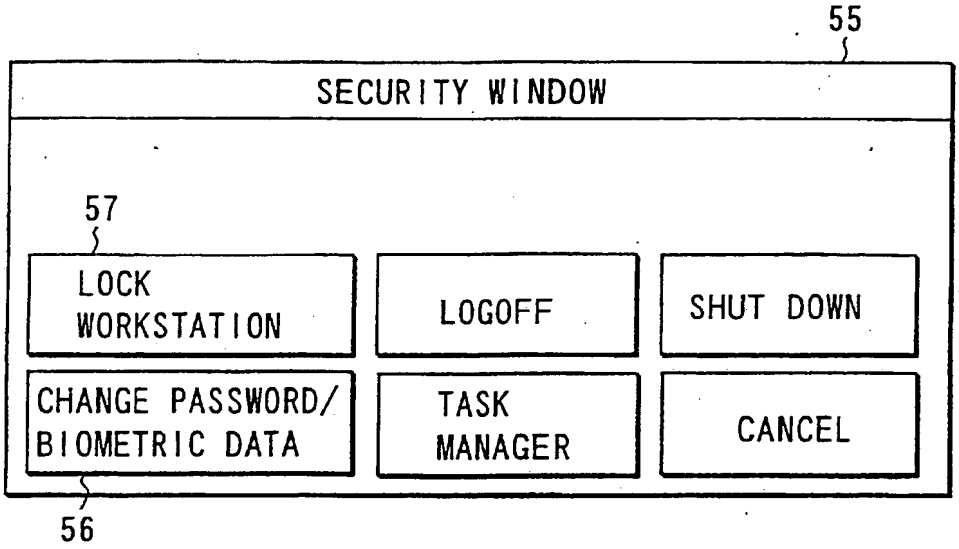

FIG. 10

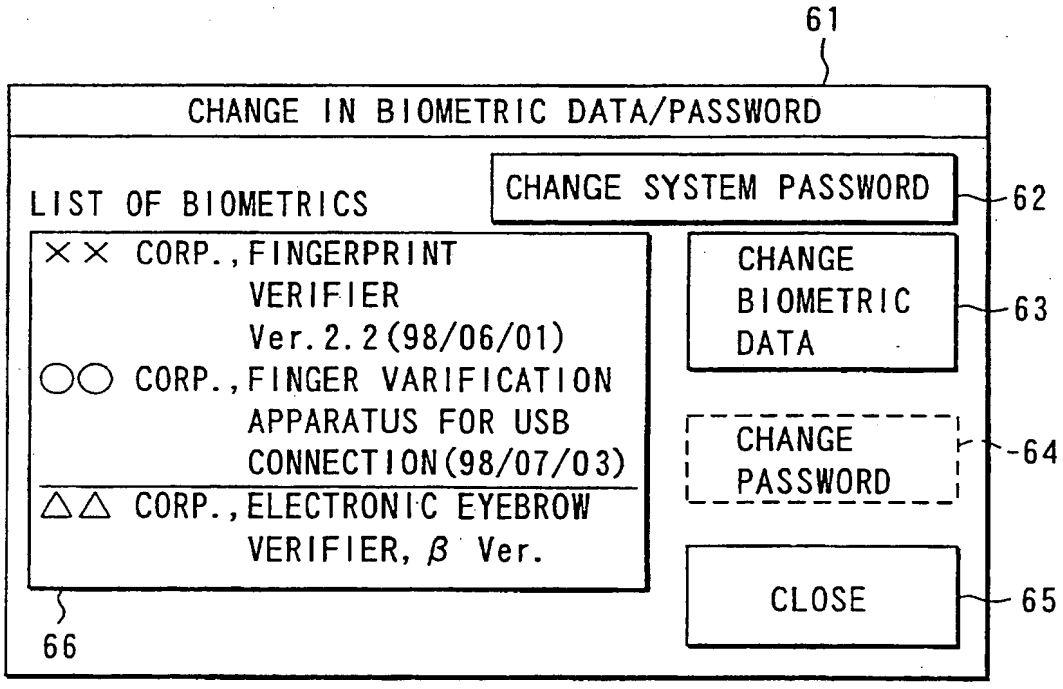

FIG. 11

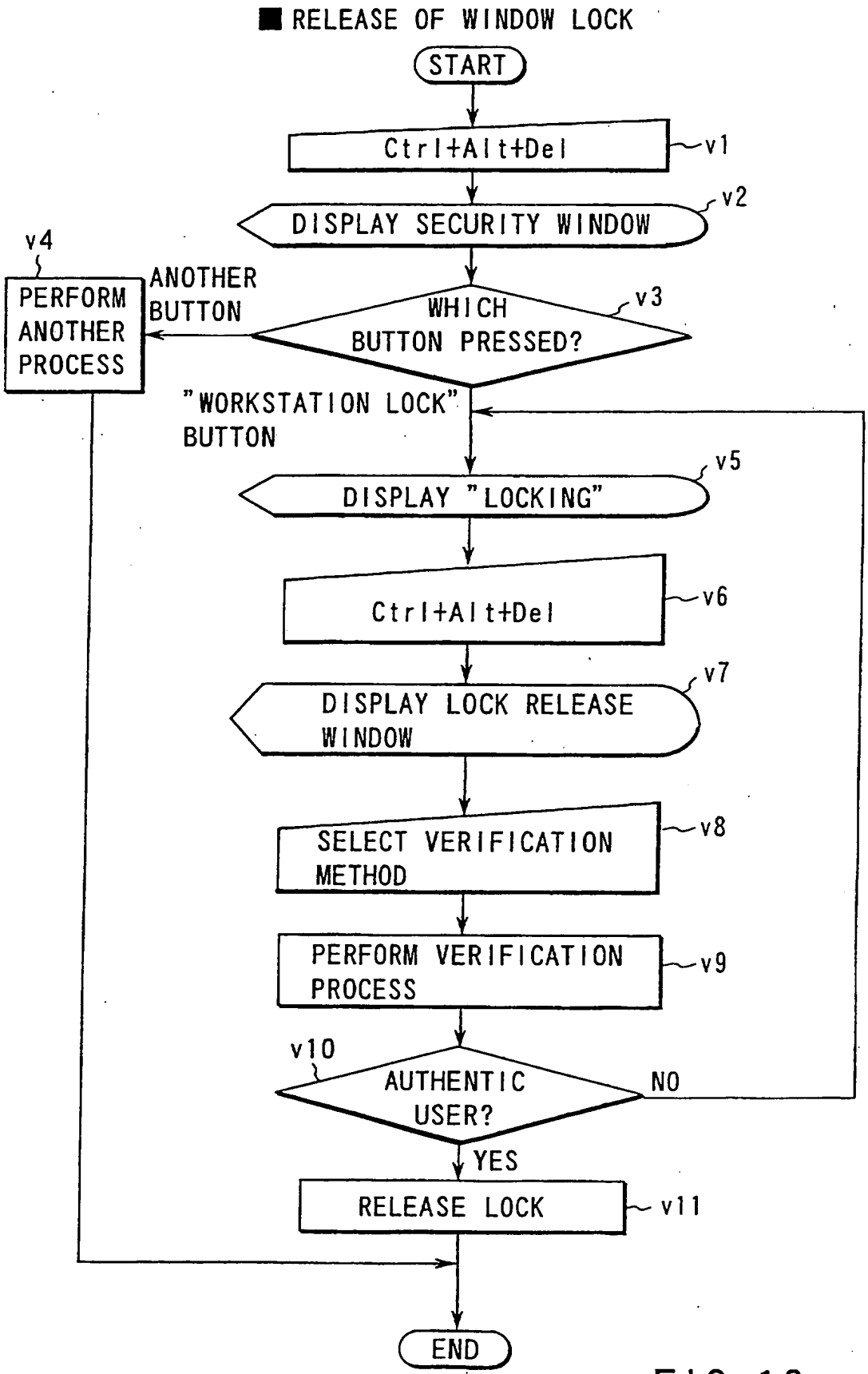

FIG. 12

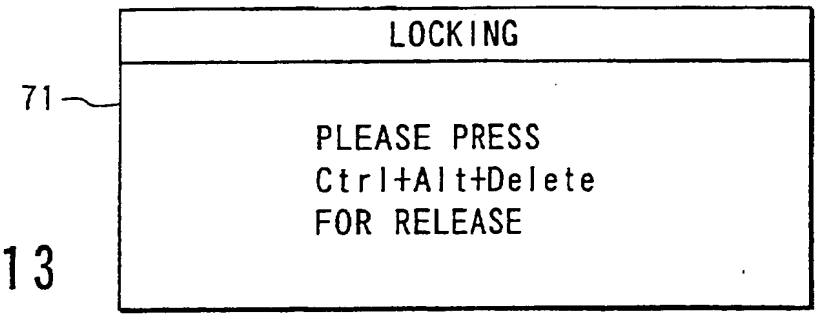

FIG. 13

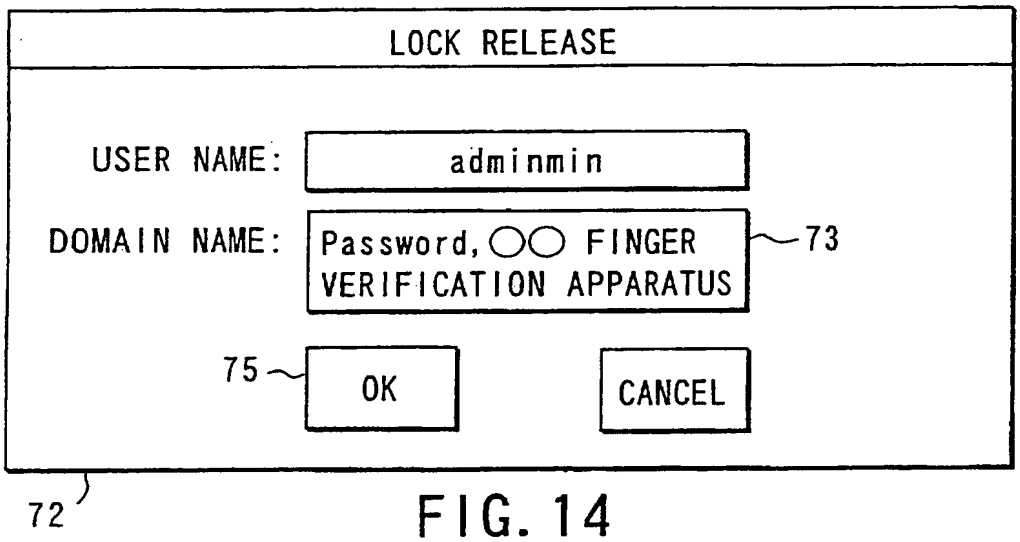

FIG. 14

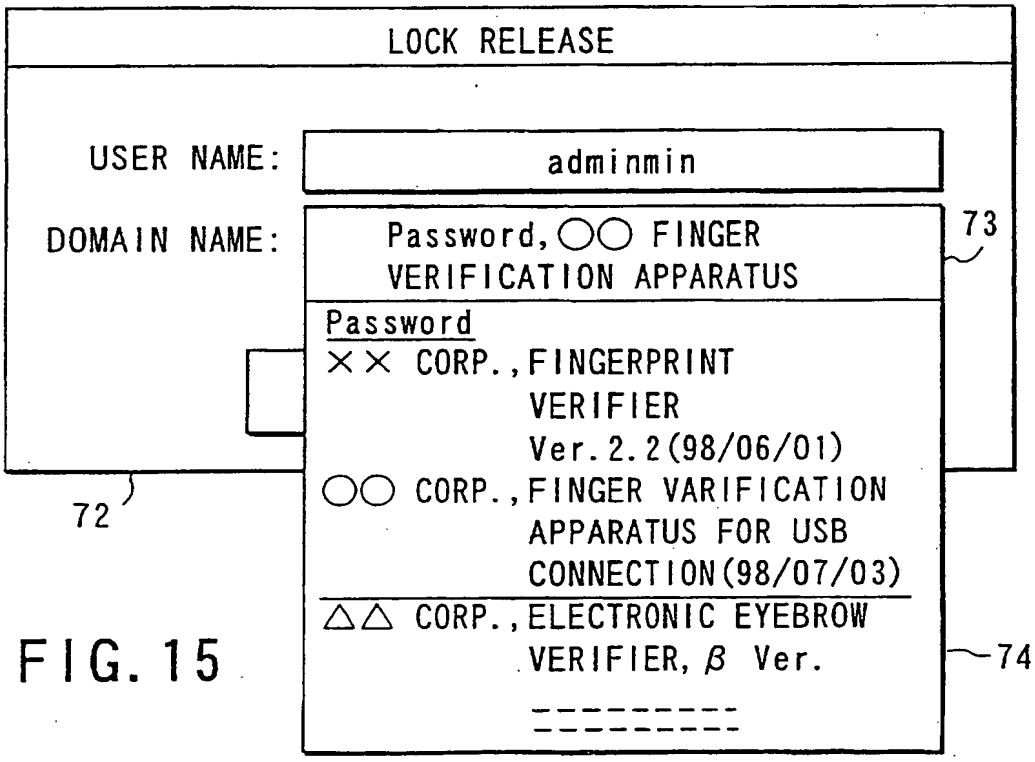

FIG. 15

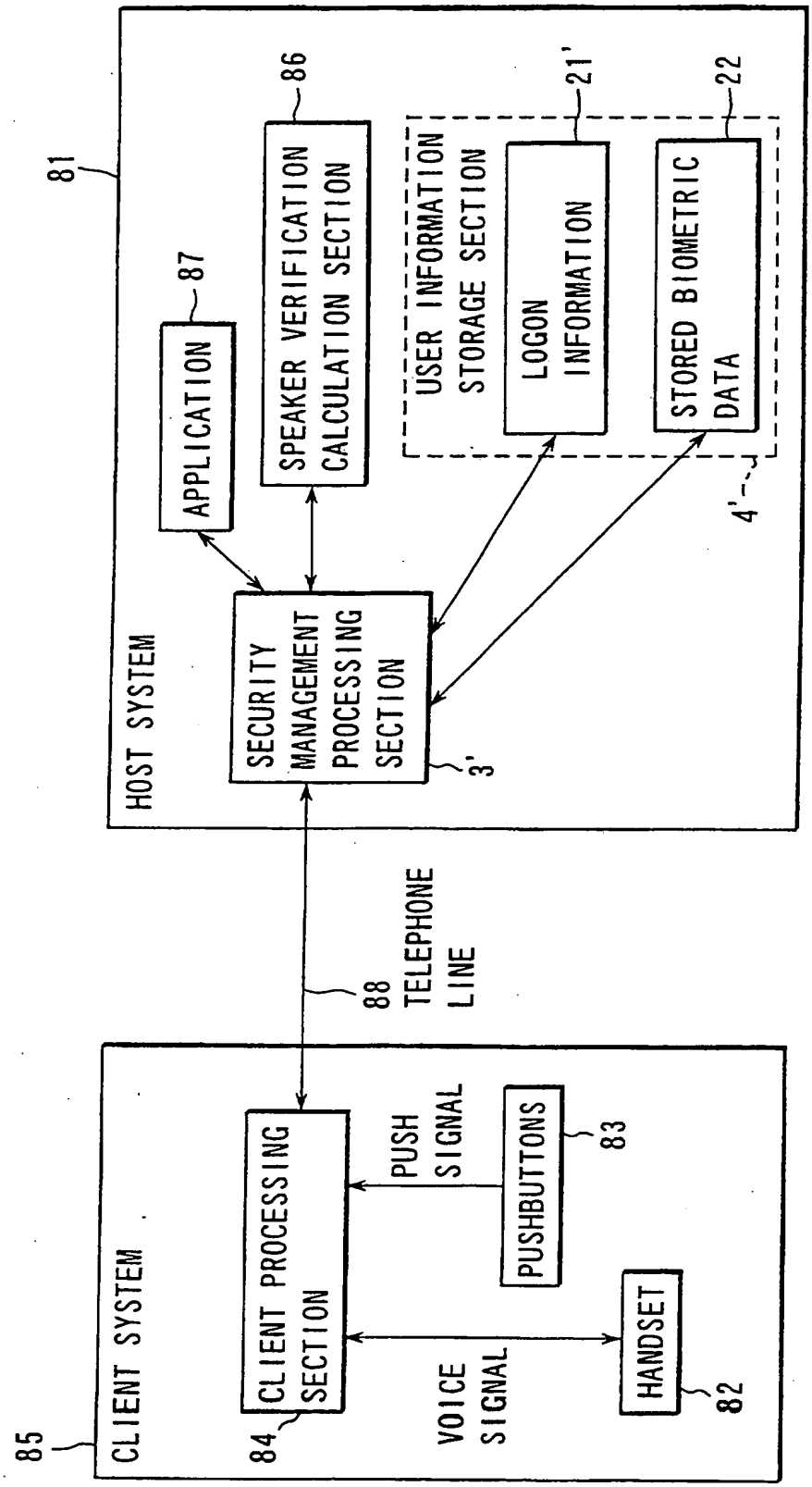

FIG. 16

■ LOGON VIA HANDSET

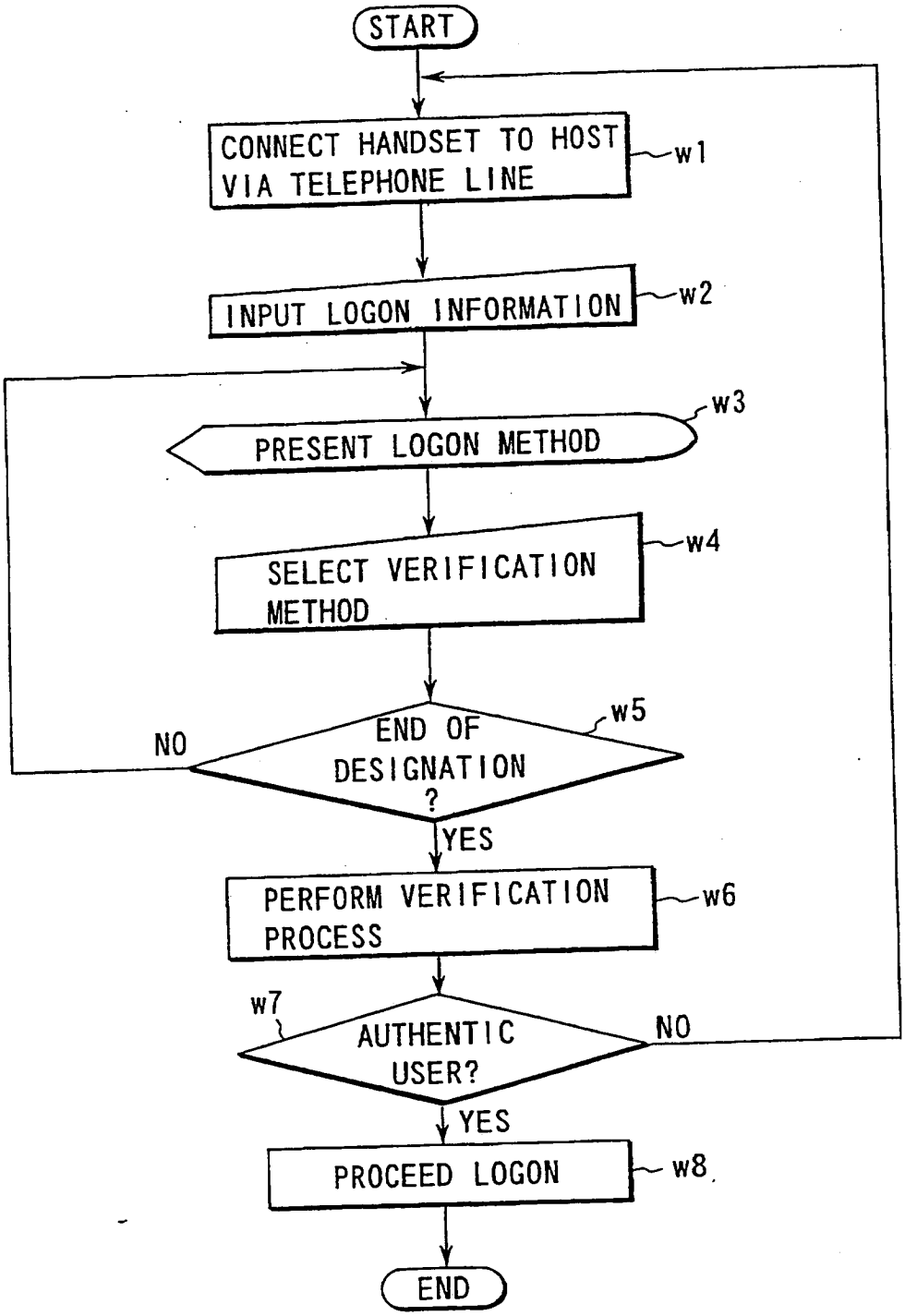

FIG. 17

TITLE OF THE INVENTION

USER CONFIRMATION SYSTEM USING BIOMETRICS AND STORAGE MEDIUM

BACKGROUND OF THE INVENTION

The present invention relates to a user confirmation system using biometrics and a storage medium.

At present, in logon to a computer and unlocking a door, an authentic user is generally confirmed using an ID card or password.

To assure system security against an illicit user or to prevent computer resources from destruction due to an accident or misuse, confidential information from leakage, or valuables from burglary, the user confirmation function has recently been increasingly important.

User confirmation systems having the above function can be used in a variety of applications such as release of screen lock in a computer, management at gates of boarders or toll roads, confirmation of cardholders of credit cards or ID cards, and confirmation of users for equipment such as heavy machinery and safes.

When a user confirmation system is constructed using an ID card, as described above, an illicit user may misuse a lost or stolen ID card. It is also difficult to avoid misuse of a card, which is falsely reported to be lost.

An attempt has been made to reduce misuse by

registering a password corresponding to each ID card. To remember the password, however, bothers the user. The user may forget the password, or a third party may read the password, which thus leads to a leakage of the password. Management using passwords is not always convenient.

In recent years, a product for entry/exit management and access control using a combination of an ID card and measurement of biometric data of fingerprints or palm patterns (biometrics) is commercially available. When the biometric data is used to confirm an authentic user, almost all problems derived from the loss or burglary of a card, the leakage or oblivion of a password, and the like can be solved.

Various makers currently provide biometric systems for various biometric data for fingerprint verification and finger verification. A user confirmation system using biometrics incorporates one of the above biometric systems.

A conventional user confirmation system using biometrics is inconvenient because a single type of biometric function is used. For example, a user confirmation system using a finger verification sensor cannot be used for a user who gets hurt in his finger.

It is difficult for conventional systems to select an appropriate biometric function depending on user conditions. That is, the conventional techniques

require design for separate user confirmation systems in units of biometric functions in order to use a plurality of biometric functions.

This problem arises from difficulty in handling biometric data integrally because the handling procedures of these data are different between the kinds of biometric functions and between system makers. It is, therefore, very cumbersome to implement a user confirmation system having a plurality of kinds of biometric functions, using the conventional techniques. Even if user confirmation systems are separately designed in units of biometric functions, they are expected to be difficult to use.

Software using biometrics is present for each biometric device. Different software applications must be used for different biometric devices. This makes it more difficult to integrally handle a plurality of biometric functions.

Under the above circumstances, it is also difficult to add a new biometric device to the existing user confirmation system or remove the current biometric device from it. To add the new biometric device or remove the current biometric device is to install or uninstall each entire system. Therefore, the conventional user confirmation system is poor in expandability and flexibility.

A conventional biometric user confirmation system

using biometric data for user verification cannot be started unless biometric data of a user as a confirmation target is registered first. Registering biometric data requires the presence of a system manager, thus imposing heavy load on the system manager.

Biometric data to be used must be announced when a user is to be confirmed in a user confirmation system. This operation may give a malicious third party a hint for user confirmation information. For example, in confirming a user, a message "please place your finger" explicitly indicates the kind of biometric function with which the user is confirmed.

As described above, since the conventional system uses a single biometric function, it is difficult to change confirmation methods depending on different authoritative levels of a general user and a system manager.

BRIEF SUMMARY OF THE INVENTION

The present invention has been made in consideration of the above situation, and has as its first object to provide a user confirmation system which allows a user to select one of a plurality of user confirmation means including a biometric system and uses biometrics to flexibly cope with an emergency that disables use of a given user confirmation means.

It is the second object of the present invention to provide a user confirmation system which uses

biometrics, and can integrally handle a plurality of user confirmation means, reduce setting operations for each individual biometric system, and increase/decrease a biometric system.

It is the third object of the present invention to provide a user confirmation system which uses biometrics allowing, e.g., use of the system even if some biometric data are not registered, making the registered biometric data secret, or setting a combination of biometric functions for each user's authoritative level.

In order to achieve the above objects according to the first aspect of the present invention, there is provided a user confirmation system using biometrics, comprising:

a plurality of types of user confirmation execution sections for confirming a user in accordance with different methods, respectively;

a confirmation method presenting section for presenting user confirmation methods respectively corresponding to the plurality of types of user confirmation execution sections; and

a management section for, when at least one of the user confirmation execution sections is selected in correspondence with the user confirmation method presented by the confirmation method presenting section, managing the selected user confirmation execution

section so as to confirm the user using the selected user confirmation execution section,

wherein at least one of the user confirmation execution sections confirms the user by measuring biometric data.

According to the present invention, the user can selectively use the plurality of user confirmation execution sections including the biometric system, and the user confirmation system can flexibly cope with an emergency that disables use of a given user confirmation execution section.

According to the second aspect of the present invention, there is provided a system of the first aspect, further comprising new confirmation method registration section for registering a new user confirmation execution section except the plurality of types of user confirmation execution sections such that the confirmation method presenting section can present the new user confirmation execution section and the management section can manage the new user confirmation execution section.

According to the present invention, the plurality of user confirmation execution sections can be integrally used, setting operation in units of individual biometric systems can be omitted, and an increase in biometric system can be managed.

According to the third aspect of the present

invention, there is provided a system of the first aspect, further comprising a confirmation method registration deleting section for deleting any one of the plurality of types of user confirmation execution sections and reflecting deletion of the user confirmation execution section on the confirmation method presenting section and the management section.

According to the present invention, the plurality of user confirmation execution sections can be integrally used, setting operation in units of individual biometric systems can be omitted, and a decrease in biometric system can be managed.

According to the fourth aspect of the present invention, there is provided a system of the first aspect, wherein when at least one of the plurality of types of user confirmation execution sections does not have biometric data, the confirmation method presenting section presents a user confirmation method corresponding to at least one of the plurality of types of user confirmation execution sections.

According to the present invention, the user confirmation system can be used even if some biometric data are not registered.

According to the fifth aspect of the present invention, there is provided a system of the first aspect, wherein when the user confirmation execution section cannot verify the user as an authentic user,

a message representing a user confirmation failure is displayed, and the message representing the user confirmation failure is the same when a confirmation failure is caused by nonregistration of biometric data in a selected user confirmation execution section and when a confirmation failure is caused by any other reason.

According to the present invention, the specific type of biometric data, which is registered in the confirmation system, can be made secret against the malicious third party.

According to the sixth aspect of the present invention, there is provided a system of the first aspect, wherein a user right is allowed or denied depending on a result of confirmation whether the user is an authentic user in the user confirmation execution section.

According to the seventh aspect of the present invention, there is provided a system of the first aspect, wherein when a plurality of user confirmation execution sections of the plurality of types of user confirmation execution sections are selected and verification success conditions are satisfied in all the selected user confirmation execution sections, a user right is allowed.

According to the present invention, security in user confirmation can be improved.

According to the eighth aspect of the present invention, there is provided a system of the first aspect, wherein the management section limits at least one of a type and number of user confirmation methods in correspondence with a user's authoritative level.

According to the present invention, a combination of biometric functions necessary for each user's authoritative level can be set. For example, in user confirmation for a system manager, security can be improved by, e.g., increasing the number of user confirmation execution sections to be selected.

According to the ninth aspect of the present invention, there is provided a system of the first aspect, wherein the user confirmation is performed for at least one of a logon to a computer, a screen lock release of a computer terminal, gate opening/closing, use of a card, and use of equipment.

According to the present invention, various user's authoritative levels can be coped with conditions to be confirmed.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out hereinafter.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention.

FIG. 1 is a block diagram showing a computer to which a user confirmation system using biometrics according to the first embodiment of the present invention is applied;

FIG. 2 is a block diagram showing the detailed arrangement of a security management processing section;

FIG. 3 is a flow chart showing a user registration process of the first embodiment;

FIG. 4 is a flow chart showing a process for confirming a user by the user confirmation system of the first embodiment and logging on to a computer;

FIG. 5 is a view showing a logon start window;

FIG. 6 is a view showing the display example of a logon information input window;

FIG. 7 is a view showing the display example of a verification method change window in the logon information input window;

FIG. 8 is a view showing the display window of

a password input window;

FIG. 9 is a flow chart showing a registration/change process for biometric data in the user confirmation system of the first embodiment;

FIG. 10 is a view showing the display example of a security window;

FIG. 11 is a view showing the display example of a biometric data/password change window;

FIG. 12 is a flow chart showing a screen lock release process using the biometrics in the user confirmation system of the first embodiment;

FIG. 13 is a view showing the display example of the window during locking;

FIG. 14 is a view showing the display example of a lock release window;

FIG. 15 is a view showing a state in which a box for selecting a verification method is opened in the lock release window;

FIG. 16 is a block diagram showing a window non-display access system to which a user confirmation system using biometrics according to the second embodiment of the present invention is applied; and

FIG. 17 is a flow chart showing a logon process using a handset in the user confirmation system of the second embodiment.

DETAILED DESCRIPTION OF THE INVENTION

Preferred embodiments of the present invention

will be described below.

(First Embodiment)

FIG. 1 is a block diagram showing a computer to which a user confirmation system using biometrics according to the first embodiment of the present invention is applied.

The user confirmation system using biometrics of this embodiment confirms users of computers (personal computers (to be also referred to as PCs) and workstations). The user confirmation system implements logon to a computer serving as a user confirmation target, screen lock release, or screen saver release.

The user confirmation system using biometrics is comprised of a computer serving as a use target upon confirmation, or computer constituent components (hardware and software) of a computer for another purpose, and a biometric sensor connected to the computer. More specifically, as shown in FIG. 1, the system is comprised of a start program 2 installed in a computer 1, security management processing section 3, user information storage section 4, biometric routine 5, and biometric verification basic routine 6 (see FIG. 2). The system also includes a biometric sensor 7 (see FIG. 2) and keyboard 8 connected to the computer 1, and computer constituent components (not shown; e.g., a mouse and display device).

The start program 2 is a system initialization

program operating first upon starting an OS (Operating System) 9 of the computer 1. The start program 2 is always ON during operation of the system. The start program 2 shifts control to the security management processing section 3 upon reception of a key command "Ctrl (Control) key + Alt key + Delete key". In this embodiment, the start program 2, the security management processing section 3, and a keyboard input device driver 10 are included in the OS 9. For example, however, the security management processing section 3 may be a program (e.g., application software or middleware) outside the OS depending on the type of OS.

The security management processing section 3 manages logon, logoff, screen lock, user change, password change, shutdown, and the like of the computer 1 and adds, deletes, and manages the biometric verification basic routine 6.

FIG. 2 is a block diagram showing the detailed arrangement of the security management processing section 3.

As shown in FIG. 2, the security management processing section 3 includes a biometric verification routine adding/deleting section 11, biometric data use/registration/change processing section 12, and display management section 13.

The biometric verification routine adding/deleting section 11 manages to additionally register or delete

the biometric verification basic routine 6 serving as an individual processing program for the biometric sensor 7 used in this system. The biometric verification routine adding/deleting section 11 also makes the biometric routine 5 verify the registered state of the routine 6. This addition or deletion allows newly installing a biometric system made up of the biometric sensor 7 and biometric verification basic routine 6 in the user confirmation system or uninstalling the biometric system from the user confirmation system.

In the system configuration shown in FIG. 1, a fingerprint verification system made up of a fingerprint verification basic routine 6a and fingerprint sensor 7a and a finger verification system made up of a finger verification basic routine 6b and finger verification sensor 7b are registered as the biometric systems.

The biometric data use/registration/change processing section 12 is comprised of a logon processing section 14 for using biometric data stored in the user information storage section 4 to confirm the user, lock processing section 15, screen saver processing section 16, and registration change processing section 17 for registering biometric data and character passwords (to be described later) in the storage section 4 or changing the biometric data stored in the storage section 4.

The biometric data use/registration/change processing section 12 receives biometric data to be registered or changed, via the biometric routine 5. The processing section 12 supplies stored biometric data 22 serving as a verification target to the biometric verification basic routine 6 via the biometric routine 5 and receives the biometric verification result. The processing sections 14 to 18 included in the biometric data use/registration/change processing section 12 execute the corresponding processes using the received biometric data and verification results.

The user information storage section 4 shown in FIGS. 1 and 2 store logon information 21 and stored biometric data 22. The logon information 21 of all the stored data is made up of a user name, logon destination, and password. The stored biometric data 22 is registered by the registration change processing section 17 such that the biometric data serving as the user confirmation target is made to correspond to the user ID.

The user management section 13 manages the input/output display window corresponding to a process to be executed by the biometric verification routine adding/deleting section 11 and biometric data use/registration/change processing section 12. The display management section 13 reads out display window

information from a display window information memory section 23 in accordance with the process of one of the processing sections 11 and 12 and displays the readout display window information on the display device. When the biometric verification routine adding/deleting section 11 additionally registers a new biometric system or deletes a biometric system, the display management section 13 reflects the change information on the display window information recorded on the display window information memory section 23.

The display management section 13 displays an error message upon the failure of a user confirmation. The same error message is displayed when the verification failure is caused by nonregistration of the biometric data in the selected user confirmation execution means such as a biometric system and when the verification failure is caused by any other reason.

The biometric routine 5 can cope with different formats and processing procedures of the data in a plurality of kinds of biometric verification basic routines 6. The biometric routine 5 serves as an interface program for exchanging data between each biometric verification basic routine 6 and the security management processing section 3 and converting data to be exchanged. The biometric routine 5 performs a conversion process so as to process the biometric verification basic routine 6 in the same data format

when viewed from the security management processing section 3.

The biometric routine 5 also executes initialization and the like of the biometric verification basic routine 6 and biometric sensor 7. For the data conversion and initialization, the biometric routine 5 receives necessary commands from the biometric verification routine adding/deleting section 11 and also receives biometric system registration information.

The biometric verification basic routine 6 has a device driver 24 for the corresponding biometric sensor 7. The routine 6 controls the corresponding biometric sensor via the device driver 24. A device driver 24a for the fingerprint sensor 7a and a device driver 24b for the finger verification sensor 7b are exemplified in FIG. 1.

The biometric verification basic routine 6 compares the biometric data read by the biometric sensor 7 with the stored biometric data 22 received via the security management processing section 3 and biometric routine 5 to verify the coincidence between these data. The verification result is output to the security management processing section 3. Upon reception of the biometric data acquisition command from the security management processing section 3, the routine 6 controls the biometric sensor 7 to acquire biometric data and sends the acquired data to

the processing section 3.

The biometric sensor 7 acquires the corresponding biometric data under the control of the biometric verification basic routine 6. In addition to the sensors 7a and 7b shown in FIG. 1, various measuring devices such as a CCD camera for acquiring image biometric data such as face shapes or eyebrow shapes and a voice sensor for measuring voiceprints are also available.

Various data are input form the keyboard 8 to the security management processing section 3 via the device driver 10. The user inputs, e.g., the character password described above, and various commands with the keyboard 8.

The correspondence between means in the appended claims and means of this embodiment will be described below.

The user confirmation execution section in the claims corresponds to a system made up of the biometric system, the keyboard for inputting a character password, and part of the biometric data use/registration/change processing section 12. The confirmation method presenting section corresponds to, e.g., the display management section 13. The management section corresponds to, e.g., the security processing section 3, and particularly, the biometric data use/registration/change processing section 12 and the like. A new

confirmation method registration section and confirmation method registration deleting section correspond to, e.g., the biometric verification routine adding/deleting section 11. The display management section of the claims corresponds to, e.g., the display management section 13.

The operation of the user confirmation system using biometrics of the first embodiment having the above arrangement will be described below.

<User Registration>

A user must be registered in use of this user confirmation system.

FIG. 3 is a flow chart showing a user registration process of the first embodiment.

A system manager registers a new user such that the user name and initial password are made to correspond to the user ID. At this time, personal biometric data such as fingerprint data and voice data are not registered yet. The registration information is stored in the logon information 21 by the registration change processing section 17 in the security management processing section 3 (s1).

As described above, immediately after the system manager registers a new user, or when a user does not use a specific biometric device, the personal biometric data for the specific biometric device is not registered in the system. At this time, this user

has an unavailable verification method of all usable verification methods displayed on a verification method selection window (FIG. 7) to be described later. To use an unavailable verification method, biometric data must be registered, as will be described later.

<Logon/Logoff to/from PC System Which Displays Window>

FIG. 4 is a flow chart showing a process for confirming a user in the user confirmation system of this embodiment and logging on to a computer.

In this embodiment, a personal computer (PC) is used as a computer. That is, a biometric system is registered in a PC system using inputs with a keyboard and mouse and outputs on a display to implement the logon function using biometrics.

The logon/logoff to/from a PC in which biometric data is already registered will be described. The registration and change of the biometric data will be described later.

When the power switch is turned on for logon, the system is started. A logon start window shown in FIG. 5 is displayed on the screen (t1 in FIG. 4).

FIG. 5 is a view showing the display example of a logon start window 41.

When the user presses the Delete key while keeping pressing the control key and the Alt key to start the logon process (t2 in FIG. 4).

The logon start window 41 is displayed under the

control of the start program 2. In this embodiment, the logon start input is "control key + Alt key + Delete key". The correspondence between the keys and the logon start input changes depending on systems (OSs). The logon information input window is directly displayed without displaying the logon input start window depending on OSs or settings. This will also apply to the subsequent processes to be described later.

The process in step t2 starts the PC process. The process in the security management processing section 3 (display management section 13) allows displaying a logon information input window 42 shown in FIG. 6 (t3 in FIG. 4). All display windows derived from the logon information input window 42 are under the control of the security management processing section 3. Note that to shut down the computer during operation, the input "control key + Alt key + Delete key" allows displaying a security window (to be described later), and the window can shift from the security window to the window 42 in FIG. 6 (t3 in FIG. 4).

FIG. 6 is a view showing the display example of the logon information input window.

The user inputs a user name 43 or selects a verification method (user confirmation method) 44 in accordance with the contents of the window (t4 and t5 in FIG. 4). In this embodiment, "adminmin" and "○○ finger verification apparatus" are selected as the user

name 43 and verification method 44, respectively. Note that the user is the system manager described above.

The previous logon information is displayed in the window boxes for inputting or changing information. When the same user logs on to the computer by the same method, the user can omit the input operation. Note that the box of the user confirmation method 44 can be kept blank to keep the password type information secret every time the user logs on to the computer.

In this window, other information (e.g., a domain name) required in logon can be displayed, changed, or input.

A method of changing the verification method will be described in detail below.

FIG. 7 is a view showing the display example of the verification method change window in the logon information input window.

First of all, to change the verification method, the user clicks the right end of the box displaying the verification method with a mouse to display a list 48 of the verification methods shown in FIG. 7. The verification methods in the list 48 are biometric systems registered in the system by the biometric verification routine adding/deleting section 11.

The user selects at least one method from the list 48 of the verification methods to change the verification method 44. The "Password" and "○○ finger

verification apparatus" are selected in FIG. 7, but another combination may be selected. Alternatively, the number of verification methods to be selected may be changed. The selected verification methods are known at a glance by, e.g., underlining them.

As described above, when appropriate information is input on the logon information input window 42, an "OK" button 45 is clicked with the mouse (t6 in FIG. 4). To cancel the choice, the user clicks a "cancel" button 46 with the mouse. To shut down the system, the user clicks a "shut down" button 47 with the mouse.

When the user presses the "cancel" button, the flow returns to step t2. When the "shut down" button 47 is pressed, the system is powered off (t7 in FIG. 4) to end the process. Note that the logoff from the computer can also be executed on the security window (to be described later).

When the user presses the "OK" button 45, one or a plurality of selected verification methods are executed (t8).

As shown in FIG. 6, when the "Password" and "○○ finger verification apparatus" are selected, the verification processing is executed in the order named.

To confirm the password, the password input window is displayed by the process in the display management section 13 on the basis of a command from the logon processing section 14 in the security management

processing section 3.

FIG. 8 is a view showing the display example of the password input window.

When the user inputs a password in a password box 52 of the password input window 51 with the keyboard 8, the input password is compared with the password in the logon information 21 by the logon processing section 14 in the biometric data use/registration/change processing section 12. When the input password is confirmed to be input by the authentic user, the process shifts to the next verification processing (finger verification).

In a conventional general PC, both a user name input box and a password input box are displayed in one window. According to the characteristic feature of this embodiment, these boxes are displayed in different windows because the biometrics and password are given the same importance.

Verification using a finger verification apparatus is then performed.

The logon processing section 14 in the biometric data use/registration/change processing section 12 in the security management processing section 3 reads out stored biometric data 22 from the user information storage section 4. This stored biometric data 22 is supplied to the finger verification basic routine 6b via the biometric routine 5. The logon processing

section 14 outputs a command for biometric information verification to the finger verification basic routine 6b.

The finger verification sensor 7b acquires the finger biometric data under the control of the finger verification basic routine 6b. The user places his finger on the sensor 7b. Note that the finger biometric data is exemplified. However, various methods may be employed to acquire biometric data. For example, the user speaks at a microphone to obtain a voiceprint, or the user faces a camera to acquire face information. In addition, information unique to an individual person, such as handwriting can be handled as biometrics although it is not biometric data. In this case, the user signs on a pen tablet to acquire handwriting information.

The finger verification basic routine 6b compares the biometric data acquired by the sensor 7b with the stored biometric data 22 supplied from the security management processing section 3. The verification result is reported to the logon processing section 14.

When the verification results represent the authentic user in both password verification and finger verification, the logon processing section 14 determines that the logon conditions are satisfied. When no satisfactory verification result is obtained in at least one of password verification and finger

verification, the logon processing section 14 determines that no logon conditions are satisfied (t9 in FIG. 4).

When the logon conditions are satisfied (t9 in FIG. 4), the logon processing section 14 notifies the start of logon to proceed the logon (t10 in FIG. 4). When the logon conditions are not satisfied (t9 in FIG. 4), the flow returns to step t3.

In this case, since the user is the system manager or an authorized person equivalent to the system manager, the logon to the computer is not allowed unless two or more verification methods are designated. That is, the logon to the computer is allowed only when the two verification conditions are satisfied. In this case, when the user selects only one verification method and presses the "OK" button, the system does not respond. A user can log on to the computer with a user name having the lowest authoritative level by selecting only one of the verification methods.

In this embodiment, the available verification method 44 can also be selected in user confirmation. However, when the unavailable verification method 44 is selected and the "OK" button 45 is clicked to tray to log on to the computer, the logon is always unsuccessful. In this case, a message representing that the biometric data is not registered is not displayed. The user feels that the verification is

unsuccessful because the biometric data is not registered. This allows preventing a user who illegally logs on to the system from providing information.

<Registration/Change of Biometric Data>

The user logs on to the PC system to make the security window display as needed, and clicks the password/biometric data change button to change various passwords and register and change the biometric data.

FIG. 9 is a flow chart showing a process for registering/changing the biometric data in the user confirmation system of this embodiment.

When the user inputs "control key + Alt key + Delete key" during use of the computer 1 (u1 in FIG. 9), the security management processing section 3 displays the security window (u2 in FIG. 9).

FIG. 10 is a view showing the display example of the security window.

Various buttons associated with the security are formed in a security window 55. The security management section 3 manages processes associated with this window and the buttons related to the user confirmation.

When the user clicks a password/biometric data change button 56 in the security window (u3 in FIG. 9), the biometric/password change window shown in FIG. 11 is displayed (u5 in FIG. 9). When any other button is clicked (u3 in FIG. 9), the corresponding process is

executed and ended (u4 in FIG. 9).

FIG. 11 is a view showing the display example of the biometric data/password change window.

To change or register a password, the user clicks a system password change button 62, password change button 64, or biometric data change button 63 in the biometric/password change window 61 (u6 and u7 in FIG. 9).

When the user clicks the system password change button 62 or password change button 64 (u7 in FIG. 9), the password is changed (u8 and u9 in FIG. 9). The system password change button 62 changes the system password (u8 in FIG. 9). The passwords here include a password used in the PC system, passwords used in the user confirmation system, and the like. When a "close" button 65 is pressed, the biometric/password change window 61 is closed (u7 in FIG. 9).

When the user selects one of the verification methods from a list 66 (u6 in FIG. 9) and clicks the biometric data change button 63 with a mouse (u7 in FIG. 9), the user can register or change the biometric data.

To change a password as in a case wherein the old password is requested, old biometric data is verified (u10 in FIG. 9). For example, fingerprint data of the index finger of the right hand is registered, and the user wants to change the fingerprint data to that of

the middle finger of the right hand. The fingerprint must be verified using the index finger of the right hand first, and then the fingerprint of the middle finger of the right hand is registered.

In this case, as for the processes in the system, the registration change processing section 17 sends the stored biometric data 22 to the biometric verification basic routine 6, and the verification processing instruction is output to the basic routine 6. The verification result is sent back from the basic routine 6.

When the authentic user is not confirmed in the verification process of the biometric verification basic routine 6 (u11 in FIG. 9), the registration change processing section 17 outputs a biometric data acquisition command to the basic routine 6 to read the biometric data (u12 in FIG. 9).

The read biometric data is sent to the registration change processing section 17, and the processing section 17 registers it as new stored biometric data 22 in the user information storage section 4 (u13 in FIG. 9).

In the above description, the change in biometric data is exemplified. However, even if biometric data is not registered, the biometric data is registered in the same manner as described above. In this case, a password window shown in FIG. 8 is displayed in

a verification process (u10 in FIG. 9), and a password is input to confirm the authentic user.

<Screen Lock Release of PC System Which Displays Window>

The screen lock release function by biometrics will now be described. This screen lock release function is mainly implemented by the lock processing section 15 in the security management processing section 3. Although the screen saver processing section 16 implements the screen saver release function by biometrics, a description of this process will be omitted because the function is the same as the screen lock release function.

FIG. 12 is a flow chart showing the screen lock release process by biometrics in the user confirmation system of this embodiment.

When the user inputs "control key + Alt key + Delete key" during operation of the computer 1 (v1 in FIG. 12), the security window shown in FIG. 10 is displayed (v2 in FIG. 12).

When the user presses the "lock" button 57 at the workstation (v3 in FIG. 12), the screen is locked, and a locking window 71 shown in FIG. 13 is displayed (v5 in FIG. 12). When the user presses any other button in the security window 55, the corresponding process is executed (v4 in FIG. 12).

FIG. 13 is a view showing the display example of

the window during locking.

This screen lock can be performed upon clicking the "lock" button 57 at the workstation as well as the lapse of a predetermined period in the absence of a key input. The screen lock function is often used when the user does not want a third party to operate the PC system, although the user interrupts the operation for a short period of time and resumes the operation from the interrupted state.

The user can release the screen lock by pressing the Delete key while keeping pressing the control and Alt keys (v6 in FIG. 12), thereby displaying the lock release window (v7 in FIG. 12).

FIG. 14 is a view showing the display example of the lock release window.

FIG. 15 is a view showing a state in which a box for selecting a verification method is selected in the lock release window.

Various kinds of information are displayed in a lock release window 72, as needed. The user can input only a verification method 73. As in the logon mode, the user appropriately selects the verification method 74 in a selection window 74 (FIG. 15) and clicks the "OK" button 75 to start the verification process (v8 and v9 in FIG. 12).

In this case, verification is performed using a biometric system in response to a command from the lock

processing section 15 (v9 in FIG. 12). The verification result is returned to the lock processing section 15. If the user is confirmed as the authentic user (v10 in FIG. 12), the lock processing section 15 releases the lock (v11 in FIG. 12). The normal operation window is then restored.

As described above, the user confirmation system using biometrics according to this embodiment of the present invention can freely register or delete the biometric systems. The biometric system is connected to the security management processing section 3 via the biometric routine 5. The biometric data can be verified regardless of the registered biometric systems. The user can selectively use the plurality of biometric systems. The user confirmation system can have the enhanced functions of using the system even if biometric system is not registered and allowing changes in biometric data, including the change in biometric system itself. There can be provided a convenient, flexible user confirmation system using safe biometrics.

The character password and the biometric password made up of biometric data are given the same importance. The biometric data can be registered and changed as if each individual user changed the password. The system manager need not register the biometric data in advance.

Due to the above characteristic feature of the system, the system manager need not attend when each

user registers biometric data. Each individual user can register and change the biometric data. In addition, the user can decide which one of the verification methods registered in the system is used or which password is registered and used.

For example, to access this system on a server machine via a network, signature verification is performed for a PDA client, fingerprint verification is performed for a desktop PC client, and voice verification is performed for a notebook PC client. In this manner, each individual user can decide an appropriate verification method.

In the above embodiment, one password is input. However, many confirmation passwords can be set and input, and the number of user confirmation methods to be presented can increase.

When a plurality of user confirmation methods are selected in user confirmation, the user right is allowed only when all the verification success conditions in each selected user confirmation method are satisfied, thereby increasing the security effect.

The limitations of the security level on the selection of the user confirmation method in user confirmation are generally set for each user's authoritative level.

In the user confirmation system using the biometrics, when an unregistered user confirmation

method is selected as biometric data in user confirmation, the same message as in the failure of verification with the registered biometric data is displayed. This prevents a malicious third party from a hint for decoding a confirmation password.

In this embodiment, the user confirmation system using biometrics is applied to logon to a computer, release of the screen lock of a computer terminal or release of a screen saver. The computer user can protect his own information and program and all resources obtainable using the computer from the malicious third party.

(Second Embodiment)

This embodiment implements a biometric logon function in a window nondisplay access system mainly using a voice input using a handset, a ten-key pad input, and a voice output, as in access to a computer via a telephone.

FIG. 16 is a block diagram showing a window non-display access system to which a user confirmation system using biometrics according to the second embodiment of the present invention is applied. The same reference numerals as in FIG. 1 denote the same parts in FIG. 16, and only different parts will be described below.

In this window nondisplay access system, the logon to a host system 81 for playing back a message to a

user is performed from a client system 85 made up of a telephone having a handset 82 and pushbuttons 83, and a client processing section 84 connected to the telephone.

The host system 81 of this access system is comprised of a security management processing section 3', user information storage section 4', a speaker verification calculation section 86, and application 87.

The security management processing section 3' is connected to the client processing section 84 in the client system 86 via a telephone line 88. The processing section 3' incorporates the function corresponding to the biometric routine 5 of the first embodiment. A biometric data use/change/registration processing section 17 has a control function for an access process using the telephone. The processing section 3' is arranged in the same manner as in the first embodiment.

The user information storage section 4' stores logon information 21' in place of the user name logon password 21 so as to be compatible with access using the telephone. The remaining arrangement of the section 4' is the same as in the first embodiment.

The speaker verification calculation section 86 is a section corresponding to the biometric data verification function in the biometric data basic routine 6 in FIG. 2.

The application 87 is a program for realizing services offered to the user upon confirming the

authentic user in the user confirmation system using biometrics. In this embodiment, the application 87 provides a message playback function and the like.

The client processing section 84 in the client system 85 is a section corresponding to the control function for the biometric sensor 7 in the biometric data basic routine 6 in FIG. 2.

The telephone having the handset 82 and the pushbuttons 83 corresponds to the biometric sensor 7 in FIG. 2. This telephone may be a cellar telephone or PHS.

As described above, the constituent components of this embodiment can be made to correspond to those of the first embodiment although the system application target is different from that of the first embodiment.

The operation of the user confirmation system using biometrics in the above arrangement according to this embodiment will be described below.

FIG. 17 is a flow chart showing a logon process using the handset in the user confirmation system of this embodiment.

A call is made from the telephone to a message playback telephone number. The telephone is connected to the host system 81 via the telephone line 88 (w1). Logon information is then input (w2).

The conversation using voices and push signals is made between the client system 85 and host system.

Upon confirming the user as the authentic user, the message to the user is played back (w3 to w8). In this example, two verification operations, i.e., password verification and speaker verification are exemplified.

A voice message "logon is made to the message system of Mr. ○○. Please press "1" and "#" for the password, "2" and "#" for XX fingerprint verification apparatus, "3" and "#" for ○○ finger verification apparatus, "4" and "#" for ＊＊ voice verification apparatus, and "#" twice for end of selection" is announced from host system side (w3).

In response to this, the user presses "1#" with the pushbuttons 83 to select the verification method (w4).

The message "The password is currently selected. Please press "1" and "#" for cancel password selection, "2" and "#" for XX fingerprint verification apparatus, "3" and "#" for ○○ finger verification apparatus, "4" and "#" for ＊＊ voice verification apparatus, and "#" twice for end of selection" is announced from host system. The host system then prompts to choice a further method (w4) or end of selection of the verification method (w3).

When the user presses "4#" with the pushbuttons 83 to select a further verification method, the following message is announced from the host system 81 (w4, w5, and w3).

The host system outputs a message "The password and ** voice verification apparatus are currently selected. Please press "1" and "#" for canceling password selection, "2" and "#" for XX fingerprint verification apparatus, "3" and "#" for ○○ finger verification apparatus, "4" and "#" for canceling selection of ** voice verification apparatus, and "#" twice for end of selection".

When the user presses "##" with the pushbuttons 83, selection of the verification method is ended (w4 and w5), and the following verification process is started (w6).

The host system outputs a message "Verification is made using the password and ** voice verification apparatus. Please input the password and then press "#"."

The user inputs "9841#" with the pushbuttons 83. The host system outputs a message "Please speak the password through the handset."

The user speaks "HIRAKE GOBOU, SAKURA SAKU HIMITSU NO JYUMONN ...." from the handset 82.

In response to the above inputs, the speaker verification calculation section 86 performs the verification process using the password and stored biometric data under the control of the security management processing section 3'. This control is similar to the first embodiment. The user is confirmed

as the authentic user (w7) to proceed the logon, and the application is executed. The following message is output from the host system to the user.

That is, the host system outputs a message "You are the right user. Three messages are played back."

As described above, the user confirmation system using biometrics according to the second embodiment of the present invention is applied to the window non-display access system having the same arrangement as that of the first embodiment, using the handset as the biometric sensor. The same effect as in the first embodiment can be obtained in the access system described above.

In each embodiment described above, a user confirmation system using biometrics is applied to the logon to a computer, release of the screen lock, and release of the screen saver, or to the window non-display access system using the telephone. However, the application targets of the present invention are not limited to the illustrated examples.

The present invention is also applicable to confirmation of an official user of computer software, entry/exit management, gate management, confirmation of a cardholder (purchase using an IC card), or user confirmation in safe use of equipment with a qualified user (for various security devices). The present invention is applied to each system described above to

obtain the same effect as described above.

A storage medium in the present invention is a storage medium which can store a program in any storage format and is accessible from a computer. Examples are a magnetic disk, floppy disk, hard disk, optical disk (e.g., CD-ROM, CD-R, or DVD), magnetooptical disk (e.g., MO), and semiconductor memory.

An OS (Operating System), middleware (e.g., database management software and network software), and the like, which operate on a computer in accordance with the instruction of a program installed from a storage medium to the computer may constitute some processes for implementing the embodiments of the present invention.

The storage media of the present invention include a medium independent of the computer, and a storage medium which stores or temporarily stores a program downloaded via a LAN or the Internet.

The number of storage media is not limited to one. When processes in the embodiments of the present invention are executed from a plurality of media, they are also included in the storage media of the present invention. The medium configuration is not limited to a specific one.

A computer according to the present invention executes each process of each embodiment on the basis of a program stored in a storage medium and can be one

device such as a personal computer or a system in which a plurality of devices are connected via a network

The computer of the present invention is not limited to a personal computer, but can be extended to any device and equipment such as an arithmetic processing unit included in an information processing device, microcomputer, and the like, all of which can implement the functions of the present invention using programs.

As has been described above, according to the present invention, there an be provided a user confirmation system which uses biometrics, allows the user to selectively use a plurality of user confirmation means having biometric systems, and can flexibly cope with an emergency that disables use of a given user confirmation means.

According to the present invention, there can also be provided a user confirmation system in which the plurality of user confirmation means can be integrally used, the time and labor required to set each individual biometric system can be reduced, and biometric systems can be increased/decreased.

According to the present invention, there can also be provided a user confirmation system which can be used even if some biometric data are not registered, can make the registered biometric data secret, and can set a combination of biometric functions necessary for

each user's authoritative level.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details and representative embodiments shown and described herein. Accordingly, various modifications may be made without departing from the spirit or scope of the general inventive concept as defined by the appended claims and their equivalents.

CLAIMS

1. A user confirmation system using biometrics, comprising:

a plurality of types of user confirmation execution sections for confirming a user in accordance with different methods, respectively;

a confirmation method presenting section for presenting user confirmation methods respectively corresponding to said plurality of types of user confirmation execution sections when the user is confirmed; and

a management section for, when at least one of said user confirmation execution sections is selected by that at least one of the user confirmation methods presented by said confirmation method presenting section is selected by the user, managing said selected user confirmation execution section so as to confirm the user using said selected user confirmation execution section,

wherein said at least one of said user confirmation execution sections confirms the user by measuring biometric data.

2. A system according to claim 1, further comprising new confirmation method registration section for registering a new user confirmation execution section except said plurality of types of user confirmation execution sections such that said confirmation

method presenting section presents the new user confirmation execution section and said management section manages the new user confirmation execution section.

3. A system according to claim 1, further comprising a confirmation method registration deleting section for deleting any one of said plurality of types of user confirmation execution sections and reflecting deletion of the user confirmation execution section on said confirmation method presenting section and said management section.

4. A system according to claim 1, wherein said confirmation method presenting section presents a user confirmation method corresponding to the at least one of said plurality of types of user confirmation execution sections regardless of whether the at least one of said plurality of types of user confirmation execution sections does not have biometric data for confirming the user.

5. A system according to claim 1, wherein when said user confirmation execution section cannot verify the user as an authentic user, a message representing a user confirmation failure is displayed, and the message representing the user confirmation failure is the same when a confirmation failure is caused by nonregistration of biometric data in a selected user confirmation execution section and when a confirmation failure is

caused by any other reason.

6. A system according to claim 1, wherein a user right is allowed or denied depending on a result of confirmation whether the user is an authentic user by said user confirmation execution section.

7. A system according to claim 1, wherein when a plurality of user confirmation execution sections of said plurality of types of user confirmation execution sections are selected and verification success conditions are satisfied in all the selected user confirmation execution sections, a user right is allowed.

8. A system according to claim 1, wherein said management section limits at least one of a type and number of user confirmation methods in correspondence with a user's authoritative level.

9. A system according to claim 1, wherein the user confirmation is performed for at least one of a logon to a computer, a screen lock release of a computer terminal, gate opening/closing, use of a card, and use of equipment.

10. A computer-readable information recording medium on which a program for controlling a user confirmation system for confirming a user as an authentic user is recorded,

said program comprising:

a plurality of types of user confirmation

execution sections for confirming a user in accordance with different methods, respectively;

a confirmation method presenting section for presenting user confirmation methods respectively corresponding to said plurality of types of user confirmation execution sections when the user is confirmed; and

a management section for, when at least one of said user confirmation execution sections is selected by that at least one of the user confirmation method presented by said confirmation method presenting section is selected by the user, managing said selected user confirmation execution section so as to confirm the user using said selected user confirmation execution section,

wherein said at least one of said user confirmation execution sections confirms the user by measuring biometric data.

11. A medium according to claim 10, further comprising new confirmation method registration section for registering a new user confirmation execution section except said plurality of types of user confirmation execution sections such that said confirmation method presenting section can present the new user confirmation execution section and said management section can manage the new user confirmation execution section.

12. A medium according to claim 10, further comprising a confirmation method registration deleting section for deleting any one of said plurality of types of user confirmation execution sections and reflecting deletion of the user confirmation execution section on said confirmation method presenting section and said management section.

13. A system according to claim 10, wherein said confirmation method presenting section presents a user confirmation method corresponding to at least one of said plurality of types of user confirmation execution sections regardless of whether the at least one of said plurality of types of user confirmation execution sections does not have biometric data for confirming the user.

14. A medium according to claim 10, wherein when said user confirmation execution section cannot verify the user as an authentic user, a message representing a user confirmation failure is displayed, and the message representing the user confirmation failure is the same when a confirmation failure is caused by nonregistration of biometric data in a selected user confirmation execution section and when a confirmation failure is caused by any other reason.

15. A medium according to claim 10, wherein a user right is allowed or denied depending on a result of confirmation whether the user is an authentic user in

said user confirmation execution section.

16. A medium according to claim 10, wherein when a plurality of user confirmation execution sections of said plurality of types of user confirmation execution sections are selected and verification success conditions are satisfied in all the selected user confirmation execution sections, a user right is allowed.

17. A medium according to claim 10, wherein said management section limits at least one of a type and number of user confirmation methods in correspondence with a user's authoritative level.

18. A medium according to claim 10, wherein the user confirmation is performed for at least one of a logon to a computer, a screen lock release of a computer terminal, gate opening/closing, use of a card, and use of equipment.

19. A computer-readable information recording medium on which a program for controlling a user confirmation system for confirming a user as an authentic user is recorded,

said program comprising:

presenting sections for presenting different user confirmation methods when the user is confirmed, wherein at least one of said different user confirmation method uses biometric data of a user; and

a confirmation section for confirming the user by

using a user confirmation method selected.

20. A user confirmation method using biometrics, comprising:

presenting user confirmation methods respectively corresponding to a plurality of types of user confirmation execution sections when the user is confirmed, the plurality of types of user confirmation execution sections for confirming a user in accordance with different methods, respectively;

selecting at least one of said user confirmation execution sections by that at least one of the user confirmation methods presented is selected by the user; and

managing said selected user confirmation execution sections so as to confirm the user using the at least one of user confirmation execution sections selected,

wherein the at least one of said user confirmation execution sections confirms the user by measuring biometric data.

21. A user confirmation system using biometrics and storage medium, substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 9920744.1	**Examiner:**	Mike Davis
Claims searched:	1-21	**Date of search:**	14 October 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4H (HTG), G4A (AAP), H4K (KOE, KF50C, KBHG)

Int Cl (Ed.6): G06F, G07C, H04M, E05B

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2148569 A	(PHILIPS) eg abstract and page 3 lines 90-125	1,10,19,20 at least
X	WO 93/13518 A1	(DIGITAL SOUND) eg abstract, page 24 line 12 to page 25 line 17, and pages 45-46	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.